Jason R. Hull (Utah 11202)
MARSHALL OLSON & HULL, PC
Ten Exchange Place, Suite 350
Salt Lake City, UT 84111
Tel: (801) 456-7655
jhull@mohtrial.com

*Pro Hac Vice Forthcoming

J. Gerard Stranch, IV* (TN 23045)
Grayson Wells* (TN 039658)
STRANCH, JENNINGS & GARVEY, PLLC
223 Rosa L. Parks Avenue, Suite 200
Nashville, TN 37203
Tel: (615) 254-8801
gstranch@stranchlaw.com
gwells@stranchlaw.com

Attorneys for Plaintiff and Proposed Class

IN THE UNITED STATES DISTRICT COURT
DISTRICT OF UTAH

RICHARD JESKY, individually and on behalf of all others similarly situated Plaintiff, vs. HEALTHEQUITY, INC. Defendant.	**CLASS ACTION COMPLAINT WITH JURY DEMAND** Case No. _____

Richard Jesky ("Plaintiff"), individually and on behalf of all others similarly situated, and through undersigned counsel, brings this class action against HealthEquity, Inc. ("Defendant" or "HealthEquity"), and alleges, upon personal knowledge as to his own actions and his counsels' investigation, and upon information and belief as to all other matters, as follows:

NATURE OF THE ACTION

1. Plaintiff brings this class action lawsuit against Defendant for its failure to properly secure and safeguard Plaintiff's and other similarly situated current and former clients of Defendant HealthEquity (collectively defined herein as the "Class" or "Class Members") personally identifiable information ("PII"), including names, addresses, dates of birth, phone numbers, Social Security numbers, and financial information and other records (collectively, the "Private Information") from cybercriminals.

2. HealthEquity provides a health care savings account to individuals and businesses in the United States. HealthEquity serves as the custodian of Health Savings Accounts and other similar types of accounts[1]

3. Plaintiff and Class Members' sensitive personal information—which they entrusted to Defendant on the mutual understanding that Defendant would protect against disclosure—was targeted, compromised, and unlawfully accessed due to the Data Breach.

4. As part of its business, Defendant collects a treasure-trove of data from their HealthEquity clients, including highly sensitive Private Information.

5. Providers of health care savings accounts that handle Private Information have an obligation to employ reasonable and necessary data security practices to protect the sensitive, confidential and personal information entrusted to them.

6. This duty exists because it is foreseeable that the exposure of such Private Information to unauthorized persons—and especially hackers with nefarious intentions—will result in harm to the affected individuals, including, but not limited to, financial information, identity theft, invasion of their private matters and other long-term issues.

7. The harm resulting from a data and privacy breach manifests in several ways, including identity theft and financial and medical fraud, and the exposure of a person's Private Information through a data breach ensures that such person will be at a substantially increased and certainly impending risk of identity theft crimes compared to the rest of the population, potentially for the rest of their lives.

8. Mitigating that risk requires individuals to devote significant time, money, and

[1] Richard Console, Jr., *HealthEquity Notifies 4.3 Million Consumers of March 2024 Data Breach*, JD SUPRA (July 29, 2024), https://www.jdsupra.com/legalnews/healthequity-notifies-4-3-million-9030043.

other resources to closely monitor their credit, financial accounts, and email accounts, as well as to take several additional prophylactic measures.

9. In this instance, all of that could have been avoided if Defendant had employed reasonable and appropriate data security measures.

10. HealthEquity explains that the incident resulted in an unauthorized party being able to access consumers' sensitive information, which includes their first names, last names, addresses, telephone numbers, employers & employee ID numbers, Social Security numbers, dependent information, and payment card information.[2]

11. The breach involved the divulgence of Private Information of Defendant's HealthEquity clients including their: name, contact information (e.g., email address, phone number), date of birth, Social Security number, driver's license or other government identification, and/or unique identifiers to associate individuals with HealthEquity account.

12. Because of the nature of the Private Information stolen, cybercriminals now have all the necessary ingredients to perpetrate identity theft and financial fraud crimes against Plaintiff and the proposed Class Members.

13. On March 25, 2024, HealthEquity received an alert describing a possible data security incident. In response, HealthEquity purportedly secured its network and then launched an investigation to learn more about the incident and whether any consumer information may have been impacted.

14. On June 10, 2024, HealthEquity completed its investigation, confirming that an unauthorized party had been able to access certain consumer data.[3]

[2] *See id.*
[3] *Id.*

15. After learning that sensitive consumer data was accessible to an unauthorized party, HealthEquity reviewed the compromised files to determine what information was leaked and which consumers were impacted.

16. HealthEquity completed this process on June 26, 2024. Although the breached information may vary depending on the individual, it may include your first name, last name, address, telephone number, employer & employee ID number, Social Security number, dependent information, and payment card information.[4]

17. Based on news reports HealthEquity mounted an investigation into the breach itself, the causes, or what specific information of Plaintiff and the proposed Class was lost to criminals.

18. Defendant's "disclosure" amounts to no real notification at all, as it fails to inform, with any degree of specificity, Plaintiff and Class Members of the Data Breach's critical facts. Without these details, Plaintiff's and Class Members' ability to mitigate the harms resulting from the Data Breach has been severely diminished.

19. As a direct and proximate result of Defendant's failure to implement and to follow basic security procedures, Plaintiff's and Class Members' Private Information now appears to be in the hands of cybercriminals.

20. Plaintiff and Class Members are now at a significantly increased and certainly impending risk of fraud, identity theft, intrusion of their privacy, Private Information being disseminated on the dark web, and similar forms of criminal mischief, risk which may last for the rest of their lives.

21. Plaintiff and Class Members have also suffered concrete injuries in fact including, but not limited to, lost or diminished value of Private Information, lost time and opportunity costs

[4] *Id.*

associated with attempting to mitigate the actual consequences of the Data Breach, loss of benefit of the bargain, lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, and actual misuse of the compromised data consisting of an increase in spam calls, texts, and/or emails.

22. Consequently, Plaintiff and Class Members must devote substantially more time, money and energy to protect themselves, to the extent possible, from these crimes. *See McMorris v. Carl Lopez & Assocs.*, 995 F.3d 295, 301 (2d Cir. 2021) (quoting *Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688, 693 (7th Cir. 2015) ("Why else would hackers break into a store's database and steal consumers' private information? Presumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities.")).

23. Plaintiff, on behalf of himself and all others similarly situated, therefore brings claims for (i) negligence; (ii) negligence *per se*; (iii) breach of an implied contract; (iv) breach of fiduciary duty; (v) invasion of privacy; (vi) unjust enrichment and (vii) declaratory judgment. Plaintiff seeks damages and injunctive relief, including the adoption of reasonably necessary and appropriate data security practices to safeguard the Private Information in Defendant's custody to prevent incidents like the Data Breach from occurring in the future.

PARTIES

Plaintiff Richard Jesky

22. Plaintiff Richard Jesky is an individual citizen residing in Olympia, Washington, where he has resided during all relevant times and intends to remain.

23. Plaintiff established a Health Savings Account with HealthEquity on or about June 10, 2021, and has continued to maintain a Health Savings Account.

24. Plaintiff understandably and reasonably believed and trusted that Plaintiff's Private

Information provided to Defendant would be kept confidential and secure and would be used only for authorized purposes, as Defendant is required to do under state and federal law.

Defendant HealthEquity, Inc.

25. Defendant, HealthEquity, is a Delaware Corporation, with its principal place of business located at 15 West Scenic Pointe Dr., Suite 100 Draper, UT 84020.

26. Established in 2002, HealthEquity is a healthcare business services company headquartered in Draper, Utah. HealthEquity serves as the custodian of Health Savings Accounts and other similar types of accounts.

27. As of July 2022, HealthEquity managed more than 7.5 million Health Savings Accounts as well as seven million other consumer-directed benefits accounts. HealthEquity is publicly traded on the Nasdaq under the symbol HQY. HealthEquity employs more than 3,126 people and generates approximately $1 billion in annual revenue.

28. According to the Defendant's website, "as part of our remarkable service, we are committed to protecting the confidentiality, integrity, and availability of your personal information and our systems and applications. This site explains our approach to securing your data against cyber threats—employing secure design and testing practices, developing a world-class Security & IT organization, and building strong partnerships across the cybersecurity industry. "[5]

JURISDICTION & VENUE

26. This Court has subject-matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2) because the amount in controversy exceeds $5 million, exclusive of interests and costs. Indeed, the Data Breach in this case reportedly affected the Private Information of 4.3 million people, so even nominal damages would place the amount in

[5] Health Equity, *Security & IT*, https://www.healthequity.com/security (last visited July 31, 2024).

controversy over $5 million. Moreover, minimal diversity exists pursuant to 28 U.S.C. § 1332(d)(2)(A) because Plaintiff Jesky is a citizen of Washington and Defendant HealthEquity is a citizen of Utah and Delaware.

27. This Court has general personal jurisdiction over HealthEquity because its headquarters is in this State, and it conducts a substantial portion of its business in this State.

28. Venue is proper in this Court under 28 U.S.C. § 1391(a)(1) because (1) a substantial part of the events giving rise to this action occurred in this District; (2) Defendant is domiciled in this District; and (3) on information and belief, Defendant's negligence and/or its willful decisions to ignore Defendant's obligations to implement reasonable, industry standard cybersecurity safeguards occurred at Defendant's Utah headquarters.

COMMON FACTUAL ALLEGATIONS

A. Defendant Collects a Significant Amount of Private Information.

29. Plaintiff and Class Members are current and former HealthEquity clients.

30. HealthEquity clients, including Plaintiff and Class Members, provided Defendant with their sensitive personally identifiable information and protected health information.

31. Upon information and belief, in the course of collecting Private Information from HealthEquity clients, including Plaintiff, Defendant promised to provide confidentiality and adequate security from the data it collected from HealthEquity clients through its applicable privacy policy and through other disclosures in compliance with statutory privacy requirements.

32. Defendant states on its website that: "We follow a defense-in-depth security model with a Joint Security Operations Center (JSOC) and Data Protection team working with security architects and engineers deploying controls designed to prevent or limit the success of an attack."[6]

[6] *Id.*

33. Defendant further states on its website that: "Our Fraud Strategy and Prevention team is leveraging the best practices of fraud prevention and cybersecurity monitoring to protect the transactions of our members and clients."[7]

34. Due to the highly sensitive and personal nature of the information Defendant acquires and stores with respect to its HealthEquity clients, Defendant is required to keep HealthEquity clients' Private Information private; comply with industry standards related to data security and the maintenance of their HealthEquity clients' Private Information; inform their HealthEquity clients of its legal duties relating to data security; comply with all federal and state laws protecting HealthEquity clients' Private Information; only use and release HealthEquity clients' Private Information for reasons that relate to the services they provide; and provide adequate notice to HealthEquity clients if their Private Information is disclosed without authorization.

35. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Defendant assumed legal and equitable duties it owed to them and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' Private Information from unauthorized disclosure and exfiltration.

36. Without the required submission of Private Information from Plaintiff and Class Members, Defendant could not perform the services it provides.

37. Plaintiff and Class Members relied on Defendant to keep their Private Information confidential and securely maintained and to only make authorized disclosures of this Information, which Defendant ultimately failed to do.

38. Defendant's actions and inactions directly resulted in the Data Breach and the

[7] *Id.*

compromise of Plaintiff's and Class Members' Private Information.

B. The Data Breach

39. On or about July 26, 2024, HealthEquity Inc. filed a notice of data breach with the Attorney General of Maine after discovering that an unauthorized party was able to access portions of its computer network.

40. In this notice, HealthEquity explains that the incident resulted in an unauthorized party being able to access consumers' sensitive information, which includes their first names, last names, addresses, telephone numbers, employers & employee ID numbers, Social Security numbers, dependent information, and payment card information. Upon completing its investigation, HealthEquity began sending out data breach notification letters to all individuals whose information was affected by the recent data security incident. [8]

41. Omitted from new releases were the identity of the cybercriminals who perpetrated this Data Breach, the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure such a breach does not occur again. To date, these omitted details have not been explained or clarified to Plaintiff and Class Members, who retain a vested interest in ensuring that their Private Information remains protected.

42. Defendant had obligations created by the FTC Act, contract, common law, state statutory law, and industry standards to keep Plaintiff's and Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

43. The Data Breach occurred as a direct result of Defendant's failure to implement and follow basic security procedures, and its failure to follow its own policies, to protect PII.

[8] *See* Console, Jr., *supra* note 1.

C. Defendant Knew the Risks of Storing Valuable Private Information & the Foreseeable Harm to Victims.

44. Defendant understood that the Private Information it collects is highly sensitive and of significant value to those who would use it for wrongful purposes.

45. Defendant also knew that a breach of its systems—and exposure of the information stored therein—would result in the increased risk of identity theft and fraud (financial and medical) against the individuals whose Private Information was compromised, as well as intrusion into their highly private information.

46. These risks are not merely theoretical; in recent years, numerous high-profile data breaches have occurred at businesses such as Equifax, Facebook, Yahoo, Marriott, Anthem as well as countless others.

47. PII has considerable value and constitutes an enticing and well-known target to hackers, who can easily sell stolen data as there has been a "proliferation of open and anonymous cybercrime forums on the Dark Web that serve as a bustling marketplace for such commerce."[9]

48. PHI, in addition to being of a highly personal and private nature, can be used for medical fraud and to submit false medical claims for reimbursement.[10]

49. The prevalence of data breaches and identity theft has increased dramatically in recent years, accompanied by a parallel and growing economic drain on individuals, businesses, and government entities.

50. In 2021 alone, there were 4,145 publicly disclosed data breaches, exposing 22

---

[9] Brian Krebs, *The Value of a Hacked Company*, Krebs on Security. KREBS ON SECURITY (July 14, 2016), http://krebsonsecurity.com/2016/07/the-value-of-a-hacked-company.

[10] *See* Brian O'Connor, *Healthcare Data Breach: What to Know About them and What to Do After One*, EXPERIAN (Mar. 31, 2023), https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one.

billion records. The United States specifically saw a ten percent increase in the total number of data breaches.[11]

51. In tandem with the increase in data breaches, the rate of identity theft complaints has also increased over the past few years; for instance, in 2017, 2.9 million people reported some form of identity fraud compared to 5.7 million people in 2021.[12]

52. Accounts that store private client information has become a prime target for threat actors: "High demand for patient information and often-outdated systems are among the nine reasons they are the biggest target for online attacks."[13]

53. Additionally, financial providers "store an incredible amount of client data. Confidential data that's worth a lot of money to hackers who can sell it quickly – making the industry a growing target."[14] [15]

54. Indeed, cybercriminals seek out PHI at a greater rate than other sources of personal information. In a 2022 report, the healthcare compliance company Protenus found that there were 905 medical data breaches in 2021, leaving over 50 million patient records exposed for 700 of the 2021 incidents. This is an increase from the 758 medical data breaches that Protenus compiled in 2020.[14]

---

[11] Flashpoint Intel Team, *New Report from Flashpoint and Risk Based Security Finds 22 Billion Records Exposed in 2021 Data Breaches* (Feb. 4, 2022), https://flashpoint.io/blog/2021-data-breach-report.

[12] Insurance Information Institute, *Facts + Statistics: Identity theft and cybercrime*, https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (last visited July 1, 2024).

[13] Swivel Secure, *9 Reasons Why Healthcare Is The Biggest Target For Cyberattacks*, https://swivelsecure.com/us/solutions/healthcare/healthcare-is-the-biggest-target-for-cyberattacks (last visited July 31, 2024).

[14] *Id.*

[15] Protenus, *Breach Barometer*, https://www.protenus.com/breach-barometer-report (last visited July 1, 2024).

55. The percentage of data breaches attributed to malicious activity rose more than five percentage points in the first six months of 2022 to account for nearly eighty percent of all reported incidents.[16]

56. The breadth of data compromised in the Data Breach makes the information particularly valuable to thieves and leaves Defendant's HealthEquity clients especially vulnerable to identity theft, tax fraud, medical fraud, credit and bank fraud and more.

57. As indicated by Jim Trainor, former second in command at the FBI's cyber security division: "Credit cards can be, say, five dollars or more where PHI records can go from $20 say up to—we've even seen $60 or $70."[17]

58. A complete identity theft kit that includes credentials may be worth up to $1,000 on the black market whereas stolen payment card information sells for more.[18] Having your records stolen can be a prescription for financial disaster. If scam artists break into networks and grab your personal information, they can impersonate you to open credit accounts, break into your bank accounts, and even blackmail you with sensitive personal details.

59. ID theft victims often must spend money to fix problems related to having their data stolen, which averages $600 according to the FTC. But security research firm Ponemon Institute found that healthcare identity theft victims spend nearly $13,500 dealing with their

---

[16] Jill McKeon, *Health Sector Suffered 337 Healthcare Data Breaches in First Half of Year*, CYBERSECURITY NEWS (July 19, 2022), https://www.techtarget.com/healthtechsecurity/news/366594713/Health-Sector-Suffered-337-Healthcare-Data-Breaches-in-First-Half-of-Year.

[17] Doug Pollack, *You Got It, They Want It* (July 29, 2015), https://www.linkedin.com/pulse/you-got-want-criminals-targeting-your-private-data-doug-pollack.

[18] *Managing cyber risks in an interconnected world, Key findings from The Global State of Information Security® Survey 2015* (Sept. 30, 2014), https://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf.

hassles, which can include the cost of paying off fraudulent medical bills.

60. Victims of data breaches may also find themselves suffering damage to their credit ratings and scores. In the worst cases, they've been threatened with losing custody of their children, been charged with drug trafficking, found it hard to get hired for a job, or even been fired by their employers.[19]

61. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity or to otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

62. In fact, as technology advances, computer programs may scan the Internet with a wider scope to create a mosaic of information that may be used to link compromised information to an individual in ways that were not previously possible. This is known as the "mosaic effect." Names and dates of birth, combined with contact information like telephone numbers and email addresses, are very valuable to hackers and identity thieves as it allows them to access users' other accounts.

63. Thus, even if certain information was not purportedly involved in the Data Breach, the unauthorized parties could use Plaintiff's and Class Members' Private Information to access

[19] Brian O'Connor, *Healthcare Data Breach: What to Know About them and What to Do After One*, Experian (Mar. 31, 2023), https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one.

accounts, including, but not limited to, email accounts and financial accounts, to engage in a wide variety of fraudulent activity against Plaintiff and Class Members.

64. For these reasons, the FTC recommends that identity theft victims take several time-consuming steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert on their account (and an extended fraud alert that lasts for 7 years if someone steals the victim's identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a freeze on their credit, and correcting their credit reports.[20] However, these steps do not guarantee protection from identity theft but can only mitigate identity theft's long-lasting negative impacts.

65. Identity thieves can also use stolen personal information such as Social Security numbers and PHI for a variety of crimes, including identity theft, credit card fraud, phone or utilities fraud, bank fraud, to obtain a driver's license or official identification card in the victim's name but with the thief's picture, to obtain government benefits, or to file a fraudulent tax return using the victim's information.

66. For example, Social Security numbers, which were compromised in the Data Breach, are among the worst kind of Private Information to have been stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as experienced by Plaintiff and some Class Members, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone

[20] *See* Federal Trade Commission, https://www.identitytheft.gov/Steps (last visited July 1, 2024).

> illegally using your Social Security number and assuming your identity can cause a lot of problems.[21]

67. What's more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

68. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[22]

69. There may be a substantial time lag between when harm occurs and when it is discovered, and between when PII is stolen and when it is misused.

70. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches: "[I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data has been sold or posted on the [Dark] Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm."[23]

71. Even if stolen PII or PHI does not include financial or payment card account

---

[21] Social Security Administration, Publication No. 05-10064, *Identity Theft and Your Social Security Number* (June 2021), https://www.ssa.gov/pubs/EN-05-10064.pdf.
[22] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back* (Feb. 9, 2015, 4:59 AM), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-hasmillionsworrying-about-identity-theft.
[23] U.S. Gov't Accountability Office, *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent is Unknown*, GAO (June 2007), https://www.gao.gov/new.items/d07737.pdf.

information, that does not mean there has been no harm, or that the breach does not cause a substantial risk of identity theft. Freshly stolen information can be used with success against victims in specifically targeted efforts to commit identity theft known as social engineering or spear phishing. In these forms of attack, the criminal uses the previously obtained PII about the individual, such as name, address, email address, and affiliations, to gain trust and increase the likelihood that a victim will be deceived into providing the criminal with additional information.

72. Based on the value of its HealthEquity clients' PII to cybercriminals, Defendant certainly knew the foreseeable risk of failing to implement adequate cybersecurity measures.

D. The Data Breach was Preventable.

73. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information they were maintaining for Plaintiff and Class Members, causing the exposure of Private Information, such as encrypting the information or deleting it when it is no longer needed. Defendant allegedly kept their data in an unsecured server with no password.

74. Defendant could have prevented this Data Breach by, among other things, properly encrypting or otherwise protecting their equipment and computer files containing Private Information.

75. To prevent and detect cyber-attacks, or to identify them quick enough to prevent exfiltration of data, Defendant should have implemented numerous measures as recommended by the United States Government and industry standards, including but not limited to:

- Implementing a cybersecurity awareness and training program.
- Enabling strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain

Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.

- Scanning all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configuring firewalls to block access to known malicious IP addresses and to IP addresses from foreign countries that are known for cyberattacks and with which Defendant does not regularly communicate.
- Regularly or continuously conducting vulnerability scans.
- Using data loss prevention and EDR/XDR technologies to identify malicious activity and data exfiltration so that such activities can be stopped.
- Using centralizing logging and alerting systems.
- Managing the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.[24]

74. Given that Defendant was storing the Private Information of its current and former HealthEquity clients, Defendant could and should have implemented all the above measures to prevent and detect cyberattacks.

75. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and data thieves acquiring and accessing the Private Information of more than eight hundred thousand individuals, including that of Plaintiff and Class Members.

[24] *How to Protect Your Networks from RANSOMWARE*, at 3, https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last visited June 7, 2024).

E. FTC Guidelines Prohibit Defendant from Engaging in Unfair or Deceptive Acts or Practices.

86. Defendant is prohibited by the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTC Act") from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission ("FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act.

87. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[25]

88. The FTC provided cybersecurity guidelines for businesses, advising that businesses should protect personal customer information, properly dispose of personal information that is no longer needed, encrypt information stored on networks, understand their network's vulnerabilities, and implement policies to correct any security problems.[26]

89. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to private data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[27]

---

[25] Federal Trade Commission, *Start with Security – A Guide for Business: Lessons Learned from FTC Cases* (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

[26] Federal Trade Commission, *Protecting Personal Information: A Guide for Business* (October 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_protecting-personalinformation.pdf.

[27] *Id.*

90. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

91. Defendant failed to properly implement basic data security practices. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to their customer data, where PII constitutes an unfair act of practice prohibited by Section 5 of the FTC Act.

92. Defendant was at all times fully aware of its obligations to protect the PII of HealthEquity clients because of its position as custodian of a health savings account, which gave it direct access to reams of customer PII. Defendant was also aware of the significant repercussions that would result from its failure to do so.

F. Defendant Violated Industry Standards.

93. Several best practices have been identified that, at a minimum, should be implemented by a custodian of Health Savings Accounts in possession of Private Information, like Defendant, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data and limiting which employees can access sensitive data. HealthEquity failed to follow these industry best practices, including a failure to implement multi-factor authentication.

94. Other best cybersecurity practices that are standard for custodian of Health Savings Accounts include installing appropriate malware detection software; monitoring and limiting the

network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

95. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

96. These foregoing frameworks are existing and applicable industry standards for custodian of Health Savings Accounts, and upon information and belief, Defendant failed to comply with at least one–or all—of these accepted standards, thereby opening the door to the threat actor and causing the Data Breach.

G. The Monetary Value of Plaintiff's & Class Members' Private Information.

97. As a result of Defendant's failures, Plaintiff and Class Members are at substantial increased risk of suffering identity theft and fraud or misuse of their Private Information.

98. From a recent study, 28% of consumers affected by a data breach become victims of identity fraud—this is a significant increase from a 2012 study that found only 9.5% of those affected by a breach would be subject to identity fraud. Without a data breach, the likelihood of identifying fraud is only about 3%.[27]

[27] Stu Sjouwerman, *28 Percent of Data Breaches Lead to Fraud*, https://blog.knowbe4.com/bid/252486/28-percent-of-data-breaches-lead-to-fraud (last visited July 1, 2024).

99. "Actors buying and selling PII from institutions and providers in underground marketplaces is very common and will almost certainly remain so due to this data's utility in a wide variety of malicious activity ranging from identity theft and financial fraud to crafting of bespoke phishing lures."[28]

100. The reality is that cybercriminals seek nefarious outcomes from a data breach to carry out a variety of crimes.[29]

101. Indeed, a robust "cyber black market" exists in which criminals openly post stolen Private Information on multiple underground Internet websites, commonly referred to as the dark web.

102. At an FTC public workshop in 2001, then-Commissioner Orson Swindle described the value of a consumer's personal information:

> The use of third-party information from public records, information aggregators and even competitors for marketing has become a major facilitator of our retail economy. Even [Federal Reserve] Chairman [Alan] Greenspan suggested here some time ago that it's something on the order of the life blood, the free flow of information.[30]

103. Commissioner Swindle's 2001 remarks are even more relevant today, as consumers' personal data functions as a "new form of currency" that supports a $26 Billion per year online advertising industry in the United States.[31]

104. The FTC has also recognized that consumer data is a new (and valuable) form of

---

[28] *Id.*
[29] Andrew Steger, *What Happens to Stolen Healthcare Data?*, HEALTHTECH (Oct. 30, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon.
[30] *Public Workshop: The Information Marketplace: Merging and Exchanging Consumer Data*, at 8:2-8 (Mar. 13, 2001), https://www.ftc.gov/sites/default/files/documents/public_events/information-marketplace-merging-and-exchanging-consumer-data/transcript.pdf.
[31] *See* Julia Angwin & Emily Steel, *Web's Hot New Commodity: Privacy* (Feb. 28, 2011, 12:01 AM), https://www.wsj.com/articles/SB10001424052748703529004576160764037920274.

currency. In an FTC roundtable presentation, another former Commissioner, Pamela Jones Harbour, underscored this point:

> Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis—and profit.[32]

105. Recognizing the high value that consumers place on their Private Information, many companies now offer consumers an opportunity to sell this information.[33] The idea is to give consumers more power and control over the type of information that they share and who ultimately receives that information. And, by making the transaction transparent, consumers will make a profit from their Private Information. This business has created a new market for the sale and purchase of this valuable data.

106. Consumers place a high value not only on their Private Information, but also on the privacy of that data. Researchers have begun to shed light on how much consumers value their data privacy, and the amount is considerable. Indeed, studies confirm that the average direct financial loss for victims of identity theft was $880.[34]

107. The value of Plaintiff's and Class Members' Private Information on the black market is substantial. Sensitive financial information can sell for as much as $363.[35]

108. This information is particularly valuable because criminals can use it to target victims with frauds and scams that take advantage of the victim's medical conditions or victim

---

[32] Statement of FTC Commissioner Pamela Jones Harbour, *Remarks Before FTC Exploring Privacy Roundtable* (Dec. 7, 2009), https://www.ftc.gov/news-events/news/speeches/remarks-ftc-exploring-privacy-roundtable.
[33] Angwin & Steel, *supra* note 31.
[34] *See* U.S. Dep't of Justice, Bureau of Justice Statistics, *Victims of Identity Theft, 2021* (Oct. 2023), https://bjs.ojp.gov/document/vit21.pdf.
[35] Center for Internet Security, *Data Breaches: In the Healthcare Sector*, CIS, https://www.cisecurity.org/blog/data-breaches-in-the-healthcare-sector (last visited July 1, 2024).

settlements. It can be used to create fake insurance claims, allowing for the purchase and resale of medical equipment, or gain access to prescriptions for illegal use or resale.

109. Financial information, in particular, is likely to be used in detrimental ways—by leveraging sensitive personal financial details to extort or coerce someone, and serious and long-term identity theft.[36]

110. "Identity theft is a great concern not only because of its rapid growth rate, but because it is the most expensive and time consuming to resolve of all types of identity theft. Additionally, identity theft is very difficult to detect which makes this form of fraud extremely dangerous."[37]

111. Identity theft can result in inaccuracies in medical records and costly false claims. It can also have life-threatening consequences. If a victim's financial information is mixed with other records, it can lead to misdiagnosis or mistreatment. "Identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[38]

112. The FTC further warns that instances of identity theft could have a negative impact on credit scores.[39]

---

[36] *Id.*
[37] Experian, *The Potential Damages and Consequences of Identity theft and Data Breaches* (Apr. 15, 2010), https://www.experian.com/innovation/thought-leadership/medical-identity-theft-healthcare-data-breaches.jsp.
[38] Michael Ollove, *The Rise of Medical Identity Theft in Healthcare*, KAISER (Feb. 7, 2014), https://khn.org/news/rise-of-indentity-theft.
[39] *What to Know About Identity Theft*, CONSUMER ADVICE, https://consumer.ftc.gov/articles/what-know-about-identity-theft (last visited July 31, 2024).

113. Here, where financial information was among the Private Information impacted in the Data Breach, Plaintiff's and Class Members' risk of suffering future identity theft is especially substantial.

114. The ramifications of Defendant's failure to keep its HealthEquity clients' Private Information secure are long-lasting and severe. Once Private Information is stolen, fraudulent use of that information and damage to victims may continue for years. Fraudulent activity might not show up for six to twelve months or even longer.

115. Approximately 21% of victims do not realize their identity has been compromised until more than two years after it has happened. This gives thieves ample time to seek multiple treatments under the victim's name. Forty percent of consumers found out they were a victim of identity theft only when they received collection letters from creditors for expenses that were incurred in their names.[40]

116. Indeed, when compromised, financial-related data is among the most private and personally consequential.[41]

117. Data breaches and identity theft, including identity theft, have a crippling effect on individuals and detrimentally impact the economy.[42]

118. At all relevant times, Defendant was well-aware, or reasonably should have been aware, that the Private Information it maintains is highly sensitive and could be used for wrongful purposes by third parties, such as identity theft (including identity theft) and fraud.

---

[40] *The Potential Damages and Consequences of Identify Theft and Data Breaches* (Apr. 15, 2010), https://www.experian.com/innovation/thought-leadership/medical-identity-theft-healthcare-data-breaches.jsp.

[41] Elinor Mills, *Study: identity theft is costly for victims* (March 3, 2010, 5:00 AM), https://www.cnet.com/news/privacy/study-medical-identity-theft-is-costly-for-victims.

[42] *Id.*

119. Upon information and good faith belief, had Defendant remedied the deficiencies in its security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, it would have prevented the cyberattack into their systems and, ultimately, the theft of the Private Information of HealthEquity clients within their systems.

120. The compromised Private Information in the Data Breach is of great value to hackers and thieves and can be used in a variety of ways. Information about, or related to, an individual for which there is a possibility of logical association with other information is of great value to hackers and thieves.

121. Indeed, "[t]here is significant evidence demonstrating that technological advances and the ability to combine disparate pieces of data can lead to identification of a consumer, computer or device even if the individual pieces of data do not constitute PII."[43] For example, different PII elements from various sources may be able to be linked in to identify an individual, or access additional information about or relating to the individual.[44]

122. Based upon information and belief, the unauthorized parties have already utilized, and will continue utilize, the Private Information they obtained through the Data Breach to obtain additional information from Plaintiff and Class Members that can be misused.

123. In addition, as technology advances, computer programs may scan the Internet with wider scope to create a mosaic of information that may be used to link information to an individual in ways that were not previously possible. This is known as the "mosaic effect."

---

[43] Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers,* FTC Report, at 20 (Mar. 2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

[44] *See id.* at 18–19 (evaluating privacy framework for entities collecting or using consumer data with can be "reasonably linked to a specific consumer, computer, or other device").

124. Names and dates of birth, combined with contact information like telephone numbers, social security numbers and email addresses, are very valuable to hackers and identity thieves as it allows them to access users' other accounts.

125. Thus, even if payment card information were not involved in the Data Breach, the unauthorized parties could use Plaintiff's and Class Members' Private Information to access accounts, including, but not limited to email accounts and financial accounts, to engage in the fraudulent activity identified by Plaintiff.

126. Given these facts, any company that transacts business with customers and then compromises the privacy of customers' Private Information has thus deprived customers of the full monetary value of their transaction with the company.

127. In short, the Private Information exposed is of great value to hackers and cyber criminals and the data compromised in the Data Breach can be used in a variety of unlawful manners, including opening new credit and financial accounts in users' names.

H. Plaintiff & Class Members Have Suffered Compensable Damages.

128. For the reasons mentioned above, Defendant's conduct, which allowed the Data Breach to occur, caused Plaintiff and Class Members significant injuries and harm in several ways.

129. The risks associated with identity theft, including identity theft, are serious. Although some identity theft victims can resolve their problems quickly, others spend hundreds to thousands of dollars and many days repairing damage to their good name and credit record. Some consumers victimized by identity theft may lose out on job opportunities, or be denied loans for education, housing or cars because of negative information on their credit reports. In rare cases, they may even be arrested for crimes they did not commit.

130. To mitigate against the risks of identity theft and fraud, Plaintiff and members of

the Class must immediately devote time, energy, and money to: 1) closely monitor their medical statements, bills, records, and credit and financial accounts; 2) change login and password information on any sensitive account even more frequently than they already do; 3) more carefully screen and scrutinize phone calls, emails, and other communications to ensure that they are not being targeted in a social engineering or spear phishing attack; and 4) search for suitable identity theft protection and credit monitoring services, and pay to procure them.

131. The need to spend this time and effort responding to Defendant's failures is particularly necessary because Defendant's failures have caused Plaintiff and the proposed Class Members to have their Social Security number stolen, which directly and greatly increases their exposure to identity theft and fraud.

132. Once Private Information is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or obtained against future misuse. For this reason, Plaintiff and Class Members will need to maintain these heightened measures for years, and possibly their entire lives because of Defendant's conduct.

133. Further, the value of Plaintiff and Class Members' PII has been diminished by its exposure in the Data Breach.

134. Plaintiff and Class Members now face a greater risk of identity theft, including medical and financial identity theft.

135. Plaintiff and Class Members are also at a continued risk because their information remains in Defendant's systems, which have already been shown to be susceptible to compromise and attack and is subject to further attack so long as Defendant fails to undertake the necessary and appropriate security and training measures to protect its HealthEquity clients' PII.

136. Plaintiff and Class Members have suffered emotional distress because of the Data

Breach, the increased risk of identity theft and financial fraud, and the unauthorized exposure of their private medical information to strangers.

137. Plaintiff and Class Members also did not receive the full benefit of their bargain when paying for medical services. Instead, they received services of a diminished value to those described in their agreements with Defendant. Plaintiff and Class Members were damaged in an amount at least equal to the difference in the value between the services they thought they paid for (which would have included adequate data security protection) and the services they actually received.

138. Plaintiff and Class Members would not have obtained services from Defendant had they known that Defendant failed to properly train its employees, lacked safety controls over its computer network, and did not have proper data security practices to safeguard their Private Information from criminal theft and misuse.

139. Finally, in addition to a remedy for the economic harm, Plaintiff and Class Members maintain an undeniable interest in ensuring that their Private Information remains secure and is not subject to further misappropriation and theft.

REPRESENTATIVE PLAINTIFF'S EXPERIENCE

Plaintiff Richard Jesky

139. Plaintiff, Jesky is a client of Defendant who started using their Health Saving Account since June 10, 2021.

140. As a condition of obtaining services from Defendant, he was required to provide his Private Information to Defendant.

141. Upon information and good faith belief, Defendant maintained Plaintiff's Private Information and financial information in its systems at the time of the Data Breach.

142. Plaintiff's is very careful about sharing his sensitive Private Information. Plaintiff stores any documents containing his Private Information in a safe and secure location. Plaintiff would not have entrusted his Private Information to Defendant had he known of Defendant's lax data security policies.

143. Because of the Data Breach, Plaintiff's made reasonable efforts to mitigate the impact of the Data Breach, including researching and verifying the legitimacy of the Data Breach, reviewing credit monitoring and identity theft protection services, and monitoring financial accounts for any unusual activity, which may take years to detect. Plaintiff has spent significant time dealing with the Data Breach—valuable time he otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

144. Plaintiff suffered actual injury from having his Private Information compromised because of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of is Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to his Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

145. Plaintiff additionally suffered actual injury in the form of his Private Information

being disseminated, on information and belief, on the dark web because of the Data Breach.

146. As a result of the Data Breach, Plaintiff's anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

147. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

148. Plaintiff, Richard Jesky has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

CLASS ALLEGATIONS

150. Plaintiff brings this class action on behalf of himself and all other individuals who are similarly situated for the Classes defined below.

151. Plaintiff seeks to represent a Nationwide Class of persons to be defined as follows:

> All individuals residing in the United States whose PII was compromised in the Defendant's Data Breach which was reported by Defendant in July 2024.

152. Excluded from the Classes are Defendant, its subsidiaries and affiliates, officers and directors, any entity in which Defendant has a controlling interest, the legal representative, heirs, successors, or assigns of any such excluded party, the judicial officer(s) to whom this action is assigned, and the members of their immediate families, all judges assigned to hear any aspect of this litigation, their immediate family members, and those individuals who make a timely and effective election to be excluded from this matter using the correct protocol for opting out.

153. This proposed class definition is based on the information available to Plaintiff currently. Plaintiff may modify the class definition in an amended pleading or when he moves for class certification, as necessary to account for any newly learned or changed facts as the situation develops and discovery gets underway.

154. **Numerosity:** Plaintiff is informed and believes, and thereon alleges, that there are at minimum, thousands of members of the Class described above. Indeed, Defendant's Data Breach reportedly affected about 4.3 million people.[45] The exact size of the Class and the identities of the individual members are identifiable through Defendant's records, including but not limited to the files implicated in the Data Breach, but based on public information, the Class includes many thousands of individuals, if not substantially more.

155. **Commonality:** This action involved questions of law and fact common to the Class that predominate over any questions affecting solely individual members of the Class. Such common questions include but are not limited to:

a. Whether Defendant failed to timely notify Plaintiff and Class Members;

b. Whether Defendant had a duty to protect the PII of Plaintiff and Class Members;

c. Whether Defendant had respective duties not to negligently, recklessly, or willfully, disclose the PII of Plaintiff and Class Members to unauthorized third parties;

d. Whether Defendant had respective duties not to disclose the PII of Plaintiff and Class Members for non-business purposes;

e. Whether Defendant failed to adequately safeguard the PII of Plaintiff and Class Members;

f. Whether and when Defendant actually learned of the Data Breach;

g. Whether Defendant was negligent in collecting and storing Plaintiff's and Class Members' PII, and breached its duties thereby;

h. Whether Defendant adequately, promptly, and accurately informed Plaintiff and

[45] Emily Olsen, *Health Equity Data Breach Could Affect 4.3M*, HEALTHCARE DIVE (July 30, 2024), https://www.healthcaredive.com/news/healthequity-data-breach-4-3-million-affected/722792.

Class Members that their PII had been compromised;

i. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class Members that their PII had been compromised;

j. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

k. Whether Defendant adequately addressed and fixed the vulnerabilities that allowed the Data Breach to occur;

l. Whether Defendant was negligent and thus caused the Data Breach;

m. Whether Defendant entered and breached an implied contract with Plaintiff and Class Members;

n. Whether Defendant was unjustly enriched;

o. Whether Plaintiff and Class Members are entitled to actual, statutory, and/or nominal damages because of Defendant's wrongful conduct; and

p. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

157. **Typicality:** Plaintiff's claims are typical of the claims of the Class. The claims of the Plaintiff and members of the Class are based on the same legal theories and arise from the same unlawful and willful conduct. Plaintiff and members of the Class were all HealthEquity clients, or family members or caregivers of HealthEquity clients, of Defendant, each having their PII exposed and/or accessed by an unauthorized third party.

158. **Policies Generally Applicable to the Class:** This class action is also appropriate for certification because Defendant acted or refused to act on grounds generally applicable to the

Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenges of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

159. **Adequacy of Representation:** Plaintiff is an adequate representative of the Class because his interests do not conflict with the interests of the members of the Class. Plaintiff will fairly, adequately, and vigorously represent and protect the interests of the members of the Class and have no interests antagonistic to the members of the Class. In addition, Plaintiff has retained counsel who are competent and experienced in the prosecution of class action litigation. The claims of Plaintiff and the Class Members are substantially identical as explained above.

160. **Superiority and Manageability:** This class action is appropriate for certification because class proceedings are superior to other available methods for the fair and efficient adjudication of this controversy and joinder of all members of the Class is impracticable. This proposed class action presents fewer management difficulties than individual litigation, and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court. Class treatment will create economies of time, effort, and expense, and promote uniform decision-making.

161. Class action Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit many Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest

claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

162. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

163. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

164. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

165. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the Private Information of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendant may

continue to act unlawfully as set forth in this Complaint.

166. Further, Defendant has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class- wide basis.

167. Likewise, particular issues are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to, those outlined in paragraph 155 *supra*.

168. **Predominance:** Common questions of law and fact predominate over any questions affecting only individual Class Members. Similar or identical violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that dominate this action. For example, Defendant's liability and the fact of damages is common to Plaintiff and each member of the Class. If Defendant breached its duty to Plaintiff and Class Members, then Plaintiff and each Class member suffered damages by that conduct.

169. **Injunctive Relief:** Defendant has acted and/or refused to act on grounds that apply generally to the Class, making injunctive and/or declaratory relief appropriate with respect to the Class. Plaintiff and the proposed Class are entitled to injunctive relief because Defendant still maintains their personally identifiable information as part of Defendant's servicing of their Health Savings Accounts, so Plaintiff and the proposed Class Members remain at risk of another Data Breach if Defendant does not implement the legally required cybersecurity protections.

170. **Ascertainability:** Members of the Class are ascertainable. Class membership is defined using objective criteria and Class Members may be readily identified through Defendant's

books and records. Indeed, the Class is readily ascertainable because Defendant was required to ascertain the individuals to whom it was statutorily required to send notice, and those are the members of the proposed Class.

CAUSES OF ACTION

COUNT I
Negligence and Negligence *Per Se*
(On behalf of Plaintiff & the Proposed Class)

171. Plaintiff restates and realleges all preceding allegations as if fully alleged herein.

172. Plaintiff brings this claim individually and on behalf of the Class.

173. Defendant owed a duty under common law to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting their PII in Defendant's possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

174. Defendant's duty to use reasonable care arose from several sources, including but not limited to those described below.

175. Defendant had a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiff and Class Members were the foreseeable and probable victims of any inadequate security practices on the part of the Defendant. By collecting and storing valuable PII that is routinely targeted by criminals for unauthorized access, Defendant was obligated to act with reasonable care to protect against these foreseeable threats.

176. Defendant's duty also arose from Defendant's position as custodian of health savings account. Defendant holds itself out as trusted providers of client health care savings accounts, and thereby assumes a duty to reasonably protect its HealthEquity clients' information. Indeed, Defendant was in a unique and superior position to protect against the harm suffered by

Plaintiff and Class Members because of the Data Breach.

177. Defendant's duty to maintain reasonable cybersecurity safeguards is moreover enshrined in Utah's Data Breach notification statute, Utah Code Ann. § 13-44-201(1), which provides for the implementation of such safeguards:

> Any person who conducts business in the state and maintains personal information shall implement and maintain reasonable procedures to: (a) prevent unlawful use or disclosure of personal information collected or maintained in the regular course of business; and (b) destroy, or arrange for the destruction of, records containing personal information that are not to be retained by the person.

178. Defendant breached the duties owed to Plaintiff and Class Members and thus were negligent. Because of Defendant's failures, which resulted in a successful attack directed towards Defendant that compromised Plaintiff's and Class Members' PII, Defendant breached its duty of care to implement reasonable cybersecurity safeguards.

179. Specifically, Defendant failed to implement sufficient logging, monitoring, and alerting systems to identify malicious or anomalous activity on its information systems, which if implemented, would have allowed Defendant to identify the attack and prevent the attackers from having the time to perform reconnaissance, identify valuable digital assets, stage those assets for exfiltration, and perform the exfiltration. These activities, which take time and effort, would have been caught and stopped before the final step of exfiltration could occur.

180. Moreover, Defendant failed to appropriately manage vendor access into its information systems. Because of its lack of supervision of its vendor's access, malicious actors were able to compromise a vendor account and then use that access to gain direct entry into Defendant's information systems. Defendant should have had systems in place to identify logins from anomalous locations and activity that was unusual for those compromised accounts. Moreover, such vendor access should require multi-factor authentication with Number Match to

identify the location from which a person with such access was requesting access from.

181. Still further, Defendant, knowing that outside vendors had access to its information systems, should have conducted tabletop exercises to ensure it was prepared to timely and appropriately respond to a compromise of vendor account credentials.

182. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and Class Members, their PII would not have been compromised. Indeed, a big part of industry standard cybersecurity controls is the ability to quickly implement incident response plans and to quickly and efficient alert administrators to malicious activity so the intrusion can be stopped before exfiltration of data occurs.

183. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have suffered injuries, including:

a. Theft of their PII, with the resulting privacy harms;

b. Costs associated with the detection and prevention of identity theft and unauthorized use of the financial accounts, including credit monitoring services;

c. Lowered credit scores due to fraudulent activity and credit inquiries they did not authorize;

d. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach, including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

e. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII being placed in the hands of criminals;

f. Damages to, and diminution in value of, their PII entrusted, directly or indirectly, to Defendant with the mutual understanding that Defendant would safeguard Plaintiff's and Class Members' data against theft and not allow access and misuse of their data by others;

g. Continued risk of exposure to hackers and thieves of their PII, which remains in Defendant's possession and is subject to further breaches so long as Defendant fail to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' data;

h. Future costs in terms of time, effort, and money that will be expended as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members;

i. The diminished value of the services they paid for and received, and

j. Emotional distress and mental anguish from the knowledge that cybercriminals bent on identity theft, fraud, and extortion now have access to their sensitive PII, including social security numbers.

k. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

184. Moreover, Defendant's conduct amounts to negligence *per se* because its failure to implement reasonable, industry standard cybersecurity safeguards is a violation of Section 5 of the FTC Act and the Utah Data Breach Notification statute.

185. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by Defendant of failing to use reasonable measures to protect Private Information. Various FTC publications and orders also form the basis of Defendant's duty.

186. Defendant violated Section 5 of the FTC Act (and similar state statutes) by failing

to use reasonable measures to protect Private Information and not complying with industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information obtained and stored and the foreseeable consequences of a data breach on Defendant's systems.

187. Defendant's violation of Section 5 of the FTC Act (and similar state statutes) constitutes negligence *per se.*

188. Class members are consumers within the class of persons Section 5 of the FTC Act (and similar state statutes) were intended to protect.

189. Moreover, the harm that has occurred is the type of harm the FTC Act (and similar state statutes) were intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiff and Class Members.

190. Furthermore, Utah's Data Breach Notification statute required Defendant to implement the same reasonable, industry standard cybersecurity safeguards. Utah Code Ann. § 13-44-201(a). The statute's primary purpose is to protect consumers from the harms that occur when defendant's failure to implement such safeguards and thus allow consumers' private information to fall into the hands of cybercriminals. It is thus precisely the type of statute that provides a basis for a negligence per se claim.

191. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and the Class, the Private Information of Plaintiff and the Class would not have been compromised.

192. There is a close causal connection between Defendant's failure to implement security measures to protect the Private Information of Plaintiff and the Class and the harm, or risk

of imminent harm, suffered by Plaintiff and the Class. The Private Information of Plaintiff and the Class was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such Private Information.

193. Additionally, as a direct and proximate result of Defendant's negligence per se, Plaintiff and the Class have suffered and will suffer the continued risks of exposure of their Private Information, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession.

194. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered because of the Data Breach.

195. Defendant's negligent conduct is ongoing, in that it still holds the Private Information of Plaintiff and Class Members in an unsafe and insecure manner.

196. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

COUNT II
Breach of Implied Contract
(*On behalf of Plaintiff & the Proposed Class*)

197. Plaintiff restates and realleges all preceding allegations as if fully alleged herein.

198. Plaintiff brings this claim individually and on behalf of the Nationwide Class.

199. When Plaintiff and Class Members provided their PII to Defendant, they entered implied contracts with Defendant, under which Defendant agreed to take reasonable steps to protect Plaintiff's and Class Members' PII, comply with their statutory and common law duties to

protect Plaintiff's and Class Members' PII, and to timely notify them in the event of a data breach.

200. Defendant solicited and invited Plaintiff and Class Members to provide their PII as part of Defendant's provision of health care savings accounts services. Plaintiff and Class Members accepted Defendant's offers and provided their PII to Defendant.

201. Implicit in the agreement between Plaintiff and Class Members and Defendant, was Defendant's obligation to: (a) use such PII for business purposes only; (b) take reasonable steps to safeguard Plaintiff's and Class Members' PII; (c) prevent unauthorized access and/or disclosure of Plaintiff's and Class Members' PII; (d) provide Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized access and/or disclosure of their PII; (e) reasonably safeguard and protect the PII of Plaintiff and Class Members from unauthorized access and/or disclosure; and (f) retain Plaintiff's and Class Members' PII under conditions that kept such information secure and confidential.

202. When entering into implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendant's data security practices complied with their statutory and common law duties to adequately protect Plaintiff's and Class Members' PII and to timely notify them in the event of a data breach.

203. Plaintiff and Class Members paid money to Defendant in exchange for services, along with Defendant's promise to protect their PII from unauthorized access and disclosure. Plaintiff and Class Members reasonably believed and expected that Defendant would use part of those funds to obtain adequate data security. Defendant failed to do so.

204. Plaintiff and Class Members would not have provided their PII to Defendant had they known that Defendant would not safeguard their PII, as promised, or provide timely notice of a data breach.

205. Plaintiff and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

206. Defendant breached its implied contracts with Plaintiff and Class Members by failing to safeguard their PII and by failing to provide them with timely and accurate notice of the Data Breach

207. The losses and damages Plaintiff and Class Members sustained, include, but are not limited to:

a. Theft of their PII;

b. Costs associated with purchasing credit monitoring and identity theft protection services;

c. Costs associated with the detection and prevention of identity theft and unauthorized use of their PII;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII being placed in the hands of criminals;

g. Damages to and diminution in value of their PII entrusted, directly or indirectly, to Defendant with the mutual understanding that Defendant would safeguard Plaintiff's and Class

Members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their PII, which remains in Defendant's possession and is subject to further breaches so long as Defendant fail to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' data;

i. Future costs in terms of time, effort, and money that will be expended as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members;

j. The diminished value of the services they paid for and received; and

k. Emotional distress from the unauthorized disclosure of PII to strangers who likely have nefarious intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiff and Class Members.

208. As a direct and proximate result of Defendant's breach of contract, Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

209. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (1) strength its data security systems and monitoring procedures; (2) submit to future annual audits of those systems and monitoring procedures; and (3) immediately provide and continue to provide adequate credit monitoring to Plaintiff and all Class Members.

COUNT II
Third-Party Beneficiary
(*On behalf of Plaintiff & the Proposed Class*)

210. Plaintiff restates and realleges all preceding allegations as if fully alleged herein.

211. HealthEquity services HSA accounts for its clients, who, on information and belief, establish contracts with HealthEquity to provide such services.

212. Such contracts were made with the express and implied understanding that the

services were being provided for Plaintiff and the proposed Class Members benefit, as they are the ones using the HSA accounts.

213. Thus, the collection and storage of the subject PII was done for the purpose of providing Plaintiff and the Class with secure financial services to pay for their various medical needs.

214. The collection and storage of Plaintiff's and Class Members' PII was done with the primary objective of providing Plaintiff and Class Members with HSA services, and they were thus the known beneficiaries of the contracts between Defendant and Plaintiff's and Class Members' employers.

215. Defendant knew that it was storing Plaintiff's and the Class' PII and was required to ensure that the data was protected as required by statutory and common law.

216. Every contract includes an implied covenant of good faith and fair dealing, which necessarily includes the understanding that the parties to the contract will perform their obligations in good faith and in accordance with the law.

217. Rather than live up to this requirement, Defendant breached its agreements with its various clients who provide HSA accounts to Plaintiff and the Class, knowing that the breach would cause widespread harm.

218. As a direct result of Defendant's failure, Plaintiff and the proposed Class Members have suffered significant privacy and economic harms, as described above, continue to be subject to such harms because their data remains both in the hands of cybercriminals and in Defendant's information systems, which remain insecure.

219. Plaintiffs are thus entitled to damages and injunctive relief.

COUNT IV
Breach of Fiduciary Duty
(On behalf of Plaintiff & the Proposed Class)

220. Plaintiff restates and realleges all preceding allegations as if fully alleged herein.

221. Given the relationship between Defendant and Plaintiff and Class members, where Defendant became a fiduciary by its undertaking and guardianship of the PII, to act primarily for Plaintiff and Class members, (1) for the safeguarding of Plaintiff and Class members' PII; (2) to timely notify Plaintiff and Class members of a Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendant did and does store.

222. Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class members upon matters within the scope of Defendant's relationship with them—especially to secure their PII.

223. Because of the highly sensitive nature of the PII, Plaintiff and Class members (or their third-party agents) would not have entrusted Defendant, or anyone in Defendant's position, to retain their PII had they known the reality of Defendant's inadequate data security practices.

224. Defendant breached its fiduciary duties to Plaintiff and Class members by failing to sufficiently encrypt or otherwise protect Plaintiff's and Class members' PII.

225. Defendant also breached its fiduciary duties to Plaintiff and Class members by failing to diligently discover, investigate, and give notice of the Data Breach in a reasonable and practicable period.

226. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiff and Class members have suffered and will continue to suffer numerous injuries (as detailed *supra*).

COUNT V
Invasion of Privacy
(On behalf of Plaintiff & the Proposed Class)

227. Plaintiff restates and realleges all preceding allegations as if fully alleged herein.

228. Plaintiff and the Class had a legitimate expectation of privacy regarding their highly sensitive and confidential PII and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

229. Defendant owed a duty to its current and former HealthEquity clients, including Plaintiff and the Class, to keep this information confidential.

230. The unauthorized acquisition (i.e., theft) by a third party of Plaintiff and Class members' PII is highly offensive to a reasonable person.

231. The intrusion was into a place or thing which was private and entitled to be private. Plaintiff and the Class (or their third-party agents) disclosed their sensitive and confidential information to Defendant, but did so privately, with the intention that their information would be kept confidential and protected from unauthorized disclosure. Plaintiff and the Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

232. The Data Breach constitutes an intentional interference with Plaintiff's and the Class's interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

233. The Data Breach furthermore represents a public disclosure of private facts in that Defendant disclosed highly sensitive and private information, including Social Security numbers, to a large population of cybercriminals that operate on the Dark Web, where they go to purchase such information to use it for extortion or identity theft/fraud.

234. Defendant acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate and, at a minimum, were substantially certain that its failure to implement reasonable, industry standard safeguards exposed Plaintiff and the proposed Class Members to privacy and economic harms. Indeed, this knowledge of substantial certain is increased because of the ubiquitous nature of cyberattacks against companies that have control over PII and/or PHI.

235. Moreover, Defendant acted with a knowing state of mind when it failed to notify Plaintiff and the Class in a timely fashion about the Data Breach, thereby materially impairing their mitigation efforts.

236. As a proximate result of Defendant's acts and omissions, the private and sensitive PII of Plaintiff and the Class were stolen by a third party and likely redisclosed to further cybercriminals through the Dark Web and Telegram channels—as that is the *modus operandi* of these types of cybergangs.[46]

237. Unless and until enjoined and restrained by order of this Court,

238. Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Class since their PII are still maintained by Defendant with their inadequate cybersecurity system and policies.

239. Plaintiff and the Class have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential records. A judgment for monetary damages will not end Defendant's inability to safeguard the PII of Plaintiff and the Class.

[46] Emily Olsen, *Health Equity Data Breach Could Affect 4.3M*, HEALTHCARE DIVE (July 30, 2024), https://www.healthcaredive.com/news/healthequity-data-breach-4-3-million-affected/722792 (reporting that "[s]ome information was also transferred off of the vendor's systems, according to a securities filing from HealthEquity early this month").

240. Defendant is liable for the privacy invasion against Plaintiff and the proposed Class members, in an amount to be determined by a jury, and which is a harm that has long been recognized at common law through Prosser's torts.

COUNT VI
Unjust Enrichment
(On behalf of Plaintiff & the Proposed Class)
(In the Alternative Pursuant to Rule 8)

241. Plaintiff restates and realleges all preceding allegations as if fully alleged herein.

242. Plaintiff brings this claim individually and on behalf of the proposed Class.

243. Upon information and belief, Defendant funded its data security measures from its general revenue including payments made by or on behalf of Plaintiff and Class Members.

244. As such, a portion of the payments made by or on behalf of Plaintiff and the Class Members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendant.

245. Plaintiff and Class Members conferred a monetary benefit on Defendant. Specifically, they opened health care savings accounts from Defendant and/or their agents and in so doing provided Defendant with their PII.

246. In exchange, Plaintiff and Class Members should have received from Defendant the goods and services that were the subject of the transaction and have their PII protected with adequate data security.

247. Defendant knew that Plaintiff and Class Members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the PII of Plaintiff and Class Members for business purposes.

248. Specifically, Defendant enriched themselves by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members PII.

Instead of providing a reasonable level of data security that would have prevented the Data Breach, Defendant instead calculated to increase its own profits and the expense of Plaintiff and Class Members by utilizing cheaper, ineffective data security measures.

249. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and Class Members because Defendant failed to implement appropriate data management and security measures that are mandated by their common law and statutory duties.

250. Defendant failed to secure Plaintiff and Class Members' PII and, therefore, did not provide full compensation for the benefit Plaintiff and Class Members conferred upon Defendant.

251. Defendant acquired Plaintiff's and Class Members' PII through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

252. If Plaintiff and Class Members knew that Defendant had not reasonably secured their PII, they would not have agreed to provide their PII to Defendant.

253. Plaintiff and Class Members have no adequate remedy at law.

254. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered injuries as detailed above.

255. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and noneconomic losses.

256. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that it unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiff and Class

Members overpaid for Defendant's services.

COUNT VII
Declaratory Judgment and Injunctive Relief
(On behalf of Plaintiff & the Proposed Class)

257. Plaintiff restates and realleges all preceding allegations as if fully alleged herein.

258. Plaintiff brings this claim individually and on behalf of the Class.

259. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as those here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

260. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiff's and Class Members' PII and whether Defendant is currently maintaining data security measures adequate to protect Plaintiff's and Class Members from further data breaches that compromise their PII. Plaintiff alleges that Defendant's data security measures remain inadequate. Furthermore, Plaintiff continues to suffer injury as a result of the compromise of his PII and remains at imminent risk that further compromises of his PII will occur in the future.

261. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendant owes a legal duty to secure HealthEquity clients' PII and to timely notify HealthEquity clients of a data breach under the common law, Section 5 of the FTC Act, and the Utah Data Breach notification statute, and

b. Defendant continues to breach this legal duty by failing to employ reasonable measures to secure HealthEquity clients' PII.

262. This Court also should issue corresponding prospective injunctive relief requiring Defendant to employ adequate security protocols consistent with law and industry standards to protect HealthEquity clients' PII.

263. If an injunction is not issued, Plaintiff will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Defendant's properties.

264. The risk of another such breach is real, immediate and substantial.

265. If another breach of Defendant's store of customer data occurs, Plaintiff will not have an adequate remedy at law because many of the resulting damages are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

266. The hardship to Plaintiff if an injunction is not issued exceeds the hardship to Defendant if an injunction is issued. Plaintiff will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Defendant of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

267. Issuance of the requested injunction will not disserve the public interest. In contrast, such an injunction would benefit the public by preventing another data breach at Defendant [what], thus eliminating the additional injuries that would result to Plaintiff and Class Members whose confidential information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and other Class Members, prays for judgment against Defendant as follows:

A. an Order certifying the Class, and appointing Plaintiff and his Counsel to represent the Class;

B. equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the Private Information of Plaintiff and Class Members;

C. injunctive relief requested by Plaintiff, including, but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members;

D. an award of all damages available at equity or law, including, but not limited to, actual, consequential, punitive, statutory and nominal damages, as allowed by law in an amount to be determined;

E. an award of attorney fees, costs, and litigation expenses, as allowed by law;

F. prejudgment interest on all amounts awarded and

G. all such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff, on behalf of himself and other members of the proposed Classes, hereby demands a jury trial on all issues so triable.

Dated: July 31, 2024

Respectfully Submitted,

MARSHALL OLSON & HULL, P.C.

By: *Jason R. Hull*
Jason R. Hull (Utah)

STRANCH, JENNINGS & GARVEY, PLLC
J. Gerard Stranch, IV
Grayson Wells

Attorneys for Plaintiff and Proposed Class